Deutsche Post

FRANKIT
New Generation Digital Franking

Version 1.3

15 May 2003

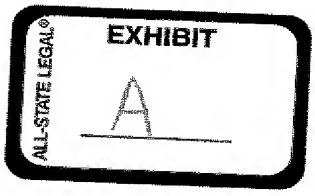
Important:
Deutsche Post is proud to provide you the English version of this document for your convenience. Please note that only the German version of this document is obliging and legally binding.

Deutsche Post AG

Headquarters

Marketing Service Products Letter Mail

53250 Bonn, Germany



Contents

be left aligned to that anchor point. Consequently, the distance between the right edge of the international variant of the barcode and the left edge of the matrix code will measure 13.25 mm. If printers are used with other resolutions than 300 dpi, the width of the barcode may vary. If a barcode must be wider than 47.25 mm, then the left edge of this barcode will move to the left, still ensuring a distance of 5 mm between the barcode's right edge and the matrix code's left edge. If the width of the code is smaller than 47.25 mm, the dimensions as stated above in the first part of this paragraph will be valid (the code will *not* move to the right). Content and specification of the barcode will be covered in section 7.

- The big letter "**R**" is used as to indicate additional services. The text must be in sans serif, regular-style Arial font with an uppercase letter height of 11.0 mm, resulting in a width of 10 mm. The distance between the left edge of the character and the left edge of the barcode measures 15 mm. This distance ensures that there is a minimum blank space of 5 mm left of the barcode.
- There is a 1-pt strong **line or stroke** above the barcode, which has the same width as the barcode used (i.e., 47.25 or 39 mm). The center of the stroke is 1 mm above the upper edge of the barcode.
- **The barcode content** is repeated in plain text above the line or stroke over the barcode. Text must be in sans serif, regular-style Arial font with an uppercase letter height of 2.0 mm. The distance between the center of the stroke and the lower edge of the plain text line is 1 mm, which means that the distance between the lower edge of the plain text line and the upper edge of the barcode is 2 mm. The plain text line starts 7 mm right of the left edge of the barcode. This position will ensure that plain text is almost centered over both the domestic and international versions of the barcode. For improved readability, plain text information is grouped. The first group holds two uppercase letters. The second group, consisting of two digits, follows after two blank spaces. The following two groups of three digits each are both separated by one blank space. After another two blank spaces, a three-character group follows, which contains the check number and two letters for the country code. Only in the case of domestic additional services does a final group of three digits containing the product code follow, again separated by two blank spaces.
- The **additional services are displayed in clear text** in two lines, which are left aligned with the barcode. The distance between the lower edge of the lower line and the upper edge of the barcode measures 5.5 mm. The line space between the lower and the upper line is 3 mm. For domestic additional services, text must be in italicized, sans serif, uppercase Arial letters with an uppercase letter height of 2.0 mm. For International additional services, upper- and lowercase characters must be used in regular style, with an upper case letter height of 1.75 mm. For separation of two different additional services, two blank spaces will be introduced. If only one line is needed, the lower of both lines must be chosen. There must be a minimum distance of 3 mm between the text and the matrix code. Section 7.2 describes how the two lines have to be filled.

The franking imprint must not be printed on dark paper or very fibrous paper (such as recycled paper, because the matrix code can easily smear).

The print on the franking imprint should be in a resolution of 300 dpi and in blue ink (as per specification) and on white or other pale-colored paper.

Franking imprints printed on units working to a lower resolution may not meet quality requirements. The test requirements are applicable and must be observed.

2.5.5 Test prints

A digital franking meter can produce test prints, i.e., franking imprints which appear to be valid franking imprints but are not intended for consignments; they serve as control prints and are useful for fine adjustment of the printer.

In this case, the franking meter must ensure that Deutsche Post does not recognize such franking imprints as valid franking imprints. This is achieved by positioning the word 'MUSTER' (sample) across the matrix code. For test prints, the data contents of the matrix code must be rendered illegible, either by the inscription mentioned above or by other means. In addition, the font format for the postage amount must be set to 'strike through' to ensure the postage amount is crossed out on any such test prints produced.

Apart from real (paid) franking imprints and specially marked test prints, no nil value imprints may be produced.

2.5.6 Franking process

To create a digital franking imprint, it is necessary to select a particular product. The product is identified by a product code supplied by Deutsche Post, which is a unique code corresponding to a combination of basic product plus additional service(s). The product code is incorporated into the matrix code and into the usage profile (see sections 4.2 and 4.11).

If mail is to be franked on behalf of a third party or if a franking meter is jointly used by a third party, then the Deutsche Post's customer number (EKP no.) of the third party must be entered into the franking meter. Entering an EKP no. might also be required for using special products in the future. If Deutsche Post issues a job number for franking (no matter whether mail is franked for or by a third party or not), then the job number must be entered into the franking meter. If both EKP and job number are applicable, only the job number has to be entered. Any of these entries must be executed before starting the franking process.

If a return answer letter is franked, the recipient's postal code must be entered into the franking meter.

2.6 Hardware and software security requirements

Intrinsic franking meter security is assured by the tamper-proof, protected area within the franking meter and the "cryptographic module," which conforms to the parameters described in *FIPS PUB 140-2, level 3, Security Requirements for*

4.2 The matrix code on a franking imprint

Version 1 of the matrix code (vgl. Byte f4) contains 84 bytes: f1 to f84

Byte no.	Length	Meaning	Data content	Comments
f1, f2, f3	3	Post company (ASCII)	„DEA" (ASCII) or '44 45 41'	Deutsche Post AG

Byte no.	Length	Meaning	Data content	Comments
f4	1	Type and version of franking	'03'	Meter franking (*FRANKIT*), Version 1 The latest type and can be taken from s4 of the Service ID, see section 4.6.

Byte no.	Length	Meaning	Data content	Comments
f5	1	Version of products/prices	'XX'	The current version of products and prices has to be mentioned here. The latest version number can be taken from s5 of the Service ID, see section 4.6.

Byte no.	Length	Meaning	Data content	Comments
f6	1	Supplier identification	'XX'	Assigned by Deutsche Post to every supplier.
f7	1	Model no.	'XX'	To be used by every supplier for each new model by arrangement with Deutsche Post, starting at '01' (first model) and increasing.
f8, f9, f10	3	Model device number	'XX XX XX'	To be used by every supplier for each model, starting at '00 00 01' and increasing to 'FF FF FF'.
				Bytes f6 to f10 correspond to the franking machine serial number (i.e. the first 5 bytes of the meter ID), see section 4.1.

Byte no.	Length	Meaning	Data content	Comments
f11, f12	2	Fee or franked value	'XX XX' in the format EEECC (decimal)	Decimal representation of the franked value, currency as per currency indicator. (E = digits before and C = digits after the decimal point). Example: 0.56 Euros: decimal: 00056; hexadecimal: '00 38'

Byte no.	Length	Meaning	Data content	Comments
f13, f14	2	Franking date	'XX XX' in the format DDDYY (decimal)	Date format: decimal representation of the year in the format DDDYY, whereby "DDD" represents the current day in the year (up to 365 or 366) and "YY" represents the last two digits of the year. (Example: 24th July 2003, i.e. 205th day in the year 2003; decimal: 20503; hexadecimal: '50 17')

Byte no.	Length	Meaning	Data content	Comments
f15, f16	2	Product code	'XX XX'	The product code is used to assign the franking printout to a particular product group. A separate description of the product code and a list of product groups to use is given in section 4.8.

Byte no.	Length	Meaning	Data content	Comments
f17	1	Key phase indicator	'XX'	Only for internal post purposes. Value to be taken unaltered from the current Postage ID, see section 4.3.

Byte no.	Length	Meaning	Data content	Comments
f18	1	Currency indicator	'01'	Euro
				Value to be taken unaltered from the current Postage ID, see section 4.3.

4.7 Hash total, truncated (security information)

A hash total is formed to provide security for normal franking (see section 4.2) and the "account franking" (see section 4.9). The hash total is generated in the protected area of the franking meter using the franking data to be protected and the m_{secret} key information, which is securely stored in the protected area.

The hash total is formed within the protected area of the franking meter by combining 80 bytes of unsecured information with the 16-byte long Postage ID and a the 16 bytes of (decrypted) m_{secret} security information. Thus, in total the hash algorithm will be applied to 112 bytes of data.

When forming the hash total in order to secure a normal franking matrix code, the first 80 bytes of the matrix code (f1 to f80) have to be taken.

When forming the hash total in order to secure the account franking, the first 80 bytes of the account franking (a1 to a80) have to be taken. Although the Postage ID is already a component of the account franking, it will again be added for the creation of the hash total for reasons of consistency. So the hash total of the account franking will also be generated by combining the 80 bytes with the 16-byte long Postage ID and a the 16 bytes of unencrypted m_{secret} security information.

Digital meters must be capable of securing the account franking by creating a hash total. The hash total will only be created upon request by the Postage Point, see section 5.5.2.

SHA-1 is used for the generation of a hash total. The Secret Suffix Method has to be applied (this means that the m_{secret} security information is tagged on at the end). The first four bytes of the resultant hash total are incorporated into the matrix code as "truncated hash".

4.8 Product codes

Deutsche Post will provide the 2-byte product code in the form of a table.

Byte no.	Length	Meaning	Data content	Comments
ps1, ps2	2	Basic product with additional services (taking into account the destination, dimensions and weight)	'XX XX'	Deutsche Post will provide the supplier with a table.

Note: The product code will indicate whether or not an additional services imprint is printed together with the franking imprint. Therefore, identical combinations of basic products and additional services will require different product codes depending on the kind of imprint.

The table of product codes provided in digital form by Deutsche Post contains product codes in decimal representation, description, postage fee, additional information (size and weight), and plain text to be included in the franking imprint for all possible combinations of basic products and additional services, see section 6.4.

Year/Month	Product code	Number of frankings	Total revenue	Customer Number (EKP no.)
Date format: YYYYMM numeric in ASCII format. Example: July 2002 is represented as: 200207	'XX XX' (2 bytes) Product code of the franking marks produced (corresponds to the product code on the franking printout). Represented in half-bytes	Numerical representation of the number of given products franked in this period, in ASCII format.	Numerical representation of the total revenue for a given product during this period, in ASCII format. The last two digits are to be read as the digits after the decimal point. Currency as per currency indicator in the account franking	Numerical representation of the postal EKP customer number in ASCII format. If the franking is performed on behalf of or by a third party, then their customer number (EKP no.) should be supplied to Deutsche Post as part of this entry. If the franking is in the customer's own name, this information needs not to be given.

Example:

Year/Month	Product code	Number of frankings	Total revenue	Customer Number (EKP no.)
200207	'00 01'	110	6160	
200207	'00 02'	240	26880	
200207	'00 02'	240	26880	5111111111
200208	'00 02'	110	12320	
Etc.				

4.12 Structure of a signed licence (without Remote Setting Center)

In the model without Remote Setting Center „signed licences" are used for the authentication of both communication partners, see section 5.2.

Both signed licence of a digital meter and signed licence of the Postage Point box comprise two components:

- Data to be signed, consisting of Meter-ID, the publick key for encryption (RSA 1024 bit) and the public key for generating digital signatures (RSA 1024 bit). Due to the public exponent the keys are actuale longer than 1024 bit; this value only represents the "module" of the key.
- A digital signature of the data to be signed, applying PKCS#7.

sage (with the attribute TYPE="errorcode") which can be analyzed by the digital meter (section 4.13).

```
<P-TALK>
    <HEAD>
        <VERSION NUMBER="1.0" OWNER="DEA" USAGE="1" LANGUAGE="de"/>
        <ACTION TYPE="metersec" STEPS="6" CURRENT="2" STATUS="invalid"/>
    </HEAD>
    <BODY>
    <MESSAGE TYPE="cert" CRYPT="no" SIGNATURE="0">signed licence of the Postage Point box
P1,2PB
    </MESSAGE>
    <MESSAGE TYPE="errorcode" CRYPT="no" SIGNATURE="1">Error code</MESSAGE>
    <SIGNATURE>Digital signature of the error code</SIGNATURE>
    </BODY>
</P-TALK>
```

6.3.3 Second transmission from the digital meter to the Postage Point

6.3.3.1 Standard communication (STATUS="ok")

A series of necessary data for requesting a new amount of postage is transmitted to the Postage Point in the second transmission by the digital meter, in the following message:

```
<P-TALK>
    <HEAD>
        <VERSION NUMBER="1.0" OWNER="DEA" USAGE="1" LANGUAGE="de"/>
        <ACTION TYPE="metersec" STEPS="6" CURRENT="3" STATUS="ok"/>
    </HEAD>
    <BODY>
        <MESSAGE TYPE="yoursession" CRYPT="yes" SIGNATURE="1"> Session ID code
SK1PB</MESSAGE>
        <MESSAGE TYPE="mysession" CRYPT="yes" SIGNATURE="2">Request Key
RKPB</MESSAGE>
        <MESSAGE TYPE="stamp" CRYPT="yes" SIGNATURE="3">Account franking APB</MESSAGE>
        <SIGNATURE>Signature SigmeterSK1PB, RKPB, APB</SIGNATURE>
        <DATALOAD>
            <SUMMARY>
                <MONTH>Reference month</MONTH>
                <PRODUCT>Product code</PRODUCT>
                <NUMBER>Number of frankings</NUMBER>
                <VALUE>Total revenue</VALUE>
            </SUMMARY>
            <SUMMARY>
                <MONTH>Reference month</MONTH>
                <PRODUCT>Product code</PRODUCT>
                <NUMBER>Number of frankings</NUMBER>
                <VALUE>Total revenue</VALUE>
                <CONTRACT>Customer number of third party</CONTRACT>
            </SUMMARY>
        </DATALOAD>
    </BODY>
</P-TALK>
```

6.3.3.2 Special communication

The digital meter can cancel the entire communications session in response to an invalid message from the Postage Point or at the user's request:

```
<P-TALK>
    <HEAD>
        <VERSION NUMBER="1.0" OWNER="DEA" USAGE="1" LANGUAGE="de"/>
        <ACTION TYPE="metersec" STEPS="6" CURRENT="3" STATUS="cancel"/>
    </HEAD>
    <BODY>
```

Example:	Identification number	4	7	3	1	2	4	8	2
	Weighing factors	8	6	4	2	3	5	9	7
	Multiplication result	32	42	12	2	6	20	72	14
	Sum of multiplications	+	+	+	+	+	÷	+	= 200
	Division	200 : 11 = 18 remaining 2							
	Subtraction	11 - 2 = 9							
	Check number	**9**							

Identification number with check number 4 7 3 1 2 4 8 2 9

Product codes for the additional services imprint (only domestic)

Domestic additional services are identified by a product code, see the following table. International additional services will not be coded.

Aditional service product code	*Description (domestic)*
110	Einschreiben
111	Einschreiben Eigenhändig
112	Einschreiben Rückschein
113	Einschreiben Eigenhändig Rückschein
200	Einschreiben Einwurf